REMARKS

Claims 1-57 are pending, with claims 1, 12, 19, 23, 34, 41, 45 and 56 being independent. Claims 1-8, 10-12, 15, 19, 21, 23-30, 32-34, 37, 41, 43, 45, 48, 52 and 56 have been amended. Claims 20 and 42 have been cancelled without prejudice. No new matter has been added. Reconsideration and allowance of the above-referenced application are respectfully requested.

Rejections Under 35 U.S.C. §§ 102 & 103

Claims 1-8, 10-17, 19-30, 32-39 and 41-57 stand rejected under 35 U.S.C. §102(e) as allegedly being anticipated over U.S. Patent No. 7,178,033 issued to Garcia. Claims 9, 18, 31 and 40 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Garcia, and further in view of DeMarines (NPL "Authentica: Content Security for the Enterprise") (hereinafter "DeMarines"). These contentions are respectfully traversed.

Examiner Cervetti is thanked for the interview, which was conducted with Mr. Hunter on February 29, 2008. During the interview, claims 1, 3, 6 and 11, and the Garcia reference were discussed. Agreement was reached that Garcia does not describe synchronizing offline access keys with a client to pre-authorize offline access to a document on that client.

Claim 1 now recites, "receiving a request from a client to take an action with respect to a first electronic document; and synchronizing offline access information with the client, in response to the request, to pre-authorize the client, to allow actions by a user as a member of a group of users, by sending to the client an update to offline access information retained at the client, the update comprising a first key associated with the group, the first key being useable at the client to access a second electronic document while offline by decrypting a second key in the second electronic document." (Emphasis added.) Thus, a key used for a whole group of users can be downloaded onto the computer of a user from the group and thereafter be used to give that user access on that specific computer (in view of the user's group membership) to a secured document that is accessed for the first time on that computer while offline. As noted in the last response, a problem that can be addressed by the presently claimed subject matter relates to how a system can efficiently pre-authorize a client to allow offline access to a secured document when that document is first opened by the user when the client is offline. When the user is online, the system can automatically cache a copy of the first key (the user group key), which can then be used later on (while offline) to decrypt the second key, which can be used to decrypt a document (e.g., a document that was received in an email, but not opened until the client was offline). *See e.g.,* the Specification at ¶s 117-121, and FIG. 11. Garcia does not teach or suggest this subject matter as claimed.

Garcia does mention the use of group keys, but Garcia does not specify the process by which those group keys are updated in the event of changes to user group membership, and Garcia is clearly focused on requiring connection to a network to pass an access test when a document is opened for the first time.

> To access the contents in the encrypted data portion 112, one needs to obtain the file key to decrypt the encrypted data portion 112. To obtain the file key, one needs to be authenticated to get a user or group key and pass an access test in which at least the access rules in the security information are measured against the user's access privilege (i.e., access rights).

See Garcia at col. 8, lines 1-7 (emphasis added). This and other portions of the document security techniques of Garcia make clear that Garcia does not in any way teach or suggest pre-authorizing a client to access an electronic document for the first time when offline.

In response to similar arguments presented in the last response, the Office states, "Examiner respectfully points to col. 7, lines 20-45, where the structure of the header is described, and further states that the security portion is included in the header, thus it travels with the file, and can therefore be accessed offline." *See* 12-10-2007 Final Office Action at page 2. However, the header is part of the file itself, not offline access information sent to a client to pre-authorize the client to provide access to another document, which may not even exist at that time. As discussed during the interview, pre-authorizing a user to access a document when offline is not equivalent to pre-authorizing a client to provide offline access to a document. Thus, for all of the above reasons, independent claim 1 should be allowable over Garcia.

Independent claim 12 should be allowable over Garcia for at least similar reasons to those addressed above. In particular, Garcia fails to teach or suggest, "synchronizing offline access information with a document control server, when online, to pre-authorize offline access to an electronic document, the synchronizing comprising receiving an update to offline access information retained locally, the update comprising a first key associated with a group of users of the document control server; and allowing access to the electronic document, when offline, by performing operations comprising using the first key to decrypt a second key in the electronic document and governing actions with respect to the electronic document based on document-permissions information associated with the electronic document." (Emphasis added.)

Independent claims 23 and 34 should be allowable over Garcia based on the arguments presented above with respect to claims 1 and 12.

Independent claim 45 should be allowable over Garcia for at least similar reasons to those addressed above. In particular, Garcia fails to teach or suggest, "a document control server that synchronizes offline access information with a client in response to a client request, to pre-authorize offline access to an electronic document by sending an update to the offline access information retained at the client, the update comprising a first key associated with a group, the first key being useable at the client to access the electronic document by decrypting a second key in the electronic document; and the client that allows access to the electronic document, when offline, by a user as a member of the group, using the first key to decrypt the second key in the electronic document and governing actions with respect to the electronic document based on document-permissions information associated with the electronic document." (Emphasis added.)

Independent claim 56 should be allowable for at least similar reasons to those addressed above. In particular, Garcia fails to teach or suggest, "server means for transparently synchronizing offline access information for controlled documents to pre-authorize a client, to allow offline actions by a user as a member of a group of users, by sending to the client an update to offline access information retained at the client, the update comprising a first key associated with the group, the first key being useable at the client to access an electronic document while offline by decrypting a second key in the electronic document; and client means for accessing the electronic document using the offline access information." (Emphasis added.)

Independent claim 19 has been amended to include the features of cancelled claim 20 and now recites, "encrypting an electronic document; and incorporating into the encrypted electronic document an address of a document control server, document-permissions information, and an encryption key useable in decrypting the encrypted electronic document, the encryption key being encrypted with a key generated by, and associated with a group of users of, the document control server; wherein the encryption key comprises a session key generated by the document control server, encrypting the electronic document comprises encrypting the electronic document using a document key, and incorporating comprises incorporating into the encrypted electronic document a document security payload comprising the document key and the document-permissions information, the document security payload being encrypted using the session key." (Emphasis added.) The cited portions of Garcia (col. 11, lines 40-67, and col. 12, lines 1-65) describe the header structure 350, but say nothing about using a session key generated by the document control server, as recited in claim 19. Thus, claim 19 should be allowable over Garcia for at least this reason, and independent claim 41 should be allowable over Garcia for at least similar reasons.

DeMarines fails to cure the noted deficiencies of Garcia, even if DeMarines is combinable with Garcia (which is not conceded). Thus, each of independent claims 1, 12, 19, 23, 34, 41, 45 and 56 should be in condition for allowance. Dependent claims 2-11, 13-18, 21-22, 24-33, 35-40, 43, 44, 46-55 and 57 should be allowable based on their dependence from allowable base claims and the additional recitations they contain. For example, claims 3 and 25 recite, "wherein synchronizing offline access information with the client comprises: receiving user-group information for the user from the client; and comparing current user-group information for the user with the received user-group information for the user from the client." Nothing in Garcia teaches or suggests receiving user-group information from the client and comparing current user-group information with the received user-group information, as claimed. Thus, claims 3 and 25 should be allowable over Garcia for at least this additional reason.

Conclusion

The foregoing comments made with respect to the positions taken by the Examiner are not to be construed as acquiescence with other positions of the Examiner that have not been explicitly contested. Accordingly, the above arguments for patentability of a claim should not be construed as implying that there are not other valid reasons for patentability of that claim or other claims.

A notice of allowance is respectfully requested. In the absence of such, a telephone interview with the Examiner and the Examiner's supervisor is respectfully requested to discuss the prior art being applied. Please apply any necessary charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: March 10, 2008

William E. Hunter
Reg. No. 47,671

Fish & Richardson P.C.
PTO Customer No. **021876**
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10808739.doc